PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-007233

(43)Date of publication of application : 11.01.2002

---

(51)Int.Cl. G06F 13/00

H04L 12/66

H04L 12/22

---

(21)Application number : 2000-182015 (71)Applicant : IONOS:KK

(22)Date of filing : 16.06.2000 (72)Inventor : HOSHINO HIROICHI

---

(54) SWITCH CONNECTION CONTROLLER FOR COMMUNICATION LINE

(57)Abstract:

PROBLEM TO BE SOLVED: To enable flexible cooperation between an internal network and an external network while preventing a physical means from directly trespassing on the internal network, when accessing from the external network.

SOLUTION: A security system, which prevents unauthorized infiltration to terminals and systems decentralized by purposes by see-saw type switching technology is provided by constituting a switch connection controller for communication lines, which is interposed between the communication lines and exclusively selects a connection with one communication line and a connection with the other communication line. Thus, the external network and internal network are disconnected by the see-saw type switching technology with a control signal of an access request corresponding to a purpose, so data can be protected securely against an unauthorized action.

LEGAL STATUS [Date of request for examination] 26.04.2007

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

reflect

the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The switch connection control unit of the channel which it is placed between channels and chooses exclusively connection with the channel of one side, and connection with the channel of another side.

[Claim 2] The main control unit which performs verification and control of data, and the 1st buffer connected with the 1st channel, The 2nd buffer which is connected to said main control unit and stores a demand or data, With the 2nd switch which short-circuits and opens the 1st switch which short-circuits and opens said the 1st buffer and 2nd buffer, and said main control unit and 2nd channel, and the directions from said main control unit The switch connection control unit of the channel which consists of the switch tube system section which outputs the control signal for short-circuiting exclusively said switch of either the 1st or a 2nd.

[Claim 3] Said 1st buffer is the switch connection control unit of the channel [equipped with a verification means to verify the justification of the demand or data from the 1st channel] according to claim 1.

[Claim 4] Said main control unit is a switch connection control unit of the channel [equipped with a verification means to verify the justification of the demand or data from the 2nd channel] according to claim 1.

[Claim 5] The switch connection control unit according to claim 2 which was equipped with the 3rd buffer which stores a demand or data between a main control unit and the 2nd switch, and the 4th buffer which stores a demand or data between said 2nd channel and said 2nd switch in addition to the above.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is applied to the security in a network, and relates to an effective technique.

[0002]

[Description of the Prior Art] It is said that the spread of the Internet changes a business gestalt from the origin.

[0003] As for a data center or a provider enterprise, the crime by access unjust these days by which even ** or an end user is always connected to the Internet is prospering. Now, even an individual is pressed for installation of security by the need from the government device.

[0004] In order to prevent access to an internal network (intranet) from external networks (Internet etc.), the fire wall technique is known.

[0005] All terminals and systems are connected on physics or logic in one Rhine, and the security of such a conventional technique judged **** logically by the fire wall.

[0006]

[Problem(s) to be Solved by the Invention] With the conventional network security technique, since all terminals and systems are connected on physics or logic in one Rhine, the trouble that an unjust invasion is possible is held.

[0007] For that, it is safest to separate an external network and an internal

network. That is, since it is not connected in any situations (destructive attack etc.) in one Rhine, an unjust invasion can be defended.

[0008] However, if access to an internal network or access to an external network from an internal network is completely intercepted from an external network, the flexible employment between networks will become impossible.

[0009] That is, separating an external network and an internal network physically has a possibility that real time nature and bidirection may be spoiled.

[0010] This invention makes it a technical technical problem to enable flexible cooperation with an internal network and an external network, preventing a direct invasion into an internal network by the physical means to access from an external network.

[0011]

[Means for Solving the Problem] This invention is the switch connection control unit of the channel which it is placed between channels and chooses exclusively connection with the channel of one side, and connection with the channel of another side.

[0012] That is, the security system which uses the switching technique of a seesaw type for the terminal and system which were distributed to purpose-oriented, and prevents an unauthorized entry is offered.

[0013] The switching technique of a seesaw type enables it to protect data from

a malfeasance certainly, in order to separate physically with the control signal of an access request [/ for the purpose of the external network and the internal network].

[0014]

[Embodiment of the Invention]

[0015]

[Example] Hereafter, the gestalt of operation of this invention is explained based on a drawing.

[0016] Drawing 1 is the functional block diagram showing the concept of this invention.

[0017] As shown in drawing 1, a purpose-oriented terminal and a purpose-oriented system are classified and distributed following three.

[0018] Among this drawing, one is an internal network which holds important data and an important system, and consists of general-purpose networks which connected the computer system by the communication line. Here, the system which has the terminal or network which is not connected with a line wire including the cable or wireless indicated to be an internal network above is called internal network. Two in drawing is an external network. Network configuration components, such as a system, a terminal, or a modular jack which has the network or network where the external network is connected with the line wire

including a cable or wireless, such as the Internet network, a public network, or a dedicated line, are called external network here. 3 is a control terminal (seesaw type switching security system) for controlling the internal network and external network used as the most important element of this invention.

[0019] The control terminal 3 consists of the switch server 31, the switch tube system section 32, a buffer 33, a buffer 34, and a seesaw switching box (SSWB) 35 further. Each of these function parts are explained in full detail later.

[0020] In this system, as shown in drawing 2 , a control terminal 3 receives the demand from an external network, and has the function transmitted to an internal network. Moreover, the data of an internal network are received and it has the function transmitted to an external network. In this drawing, the seesaw switching box (SSWB) 5 is in the condition of having connected the buffer 34 with the buffer 33, in order to tell the demand signal from the external network 2 to the internal network 1.

[0021] Moreover, as shown in drawing 3 , a control terminal 3 receives the demand from an internal network, and has the function transmitted to an external network. Moreover, the data of an external network are received and it has the function transmitted to an internal network. In this drawing, the seesaw switching box (SSWB) 5 is in the condition of having connected the internal network 1 and the switch server 31, in order to tell the demand signal from the internal network

1 to the external network 2.

[0022] As a control terminal 3 is shown in drawing 4 again, in the both sides of the internal network 1 or the external network 2, it is also possible to transmit and receive a demand signal and a data signal bidirectionally.

[0023] When using it in such the bidirectional mode, a buffer 37 is infixed between the switch server 31 and the seesaw switching box (SSWB) 35, a buffer 36 is further infixed also between the internal network 1 and the seesaw switching box (SSWB) 35, and you may make it the inside of a control terminal 3 serve as a bilateral symmetry configuration to the internal network 1 and the external network 2. In this case, a buffer 36 is held until an exterior side switch (SW2) closes the demand from an internal network. Moreover, when it judges whether there are any inaccurate data in a demand from an internal network and inaccurate data are detected, it has the function of filtering which cancels the demand.

[0024] The buffer 37 has the function to hold until an interior side switch (SW2) closes the data by which the switch server 31 received the data from the external network 2, and proper processing was carried out.

[0025] About actuation of the other control terminals 3, since it is the same as that of what was explained by above-mentioned drawing 2 thru/or 3, explanation is omitted.

[0026] In addition, although only drawing 4 showed what made the inside of a control terminal 3 bilateral symmetry structure, such structure can be applied also when a control terminal 3 is used in which the mode.

[0027] Next, the configuration, the function, and its actuation of each unit in the object distributed unit (unit distributed by purpose-oriented) of this example are explained using drawing 5 .

[0028] The switch server 31 is constituted by the computer system and consists of a central processing unit (CPU), memory, external storage, an interface (I/O), etc. centering on the bus. The program is installed in external storage and a central processing unit (CPU) outputs the control-lead signal of the seesaw switching box (SSWB) 35 to the switch tube system section 32 by loading and carrying out sequential execution of the program concerned to memory.

[0029] That is, the switch server 31 performs processing according to the purpose, such as requiring required data of an internal network, or planning adjustment of the demand from the data received from the internal network, and an external network by the demand from an external network. Moreover, the control signal for changing exclusively each gate by the side of an external network and an internal network (SW1 and SW2) based on the signal of a demand, data, etc. is sent to the switch tube system section 32.

[0030] The switch tube system section 32 consists of two or more interfaces (I/O)

focusing on a central processing unit (CPU) and memory. That is, the seesaw switching box (SSWB) 35 is controlled based on the control-lead signal from the switch server 31.

[0031] Here, the switch tube system section 32 does not contact the data signal path on a network at all, but is supervising the switch server 31, a buffer 34, a buffer 33, and a seesaw switching box (SSWB), respectively, and has the role which manages the condition of a unit.

[0032] And to a buffer 34 and a buffer 33, the control signal of each mode change is sent based on the information from switch server 31 grade. To the switch server 31, the mode condition signal of the above-mentioned buffers 34 and 33 is sent again (see drawing 13 thru/or 14). Moreover, the switch change control signal from the switch server 31 to the seesaw switching box (SSWB) 35 is received, **** with the mode condition of buffers 34 and 33 is judged, and it has the function to send a switch change control signal to a seesaw switching box (SSWB).

[0033] Although buffers 33 and 34 have the almost same configuration, the point that direct continuation of the buffer 34 is carried out to the external network differs from the point that the buffer 33 is infixed between the seesaw switching box (SSWB) 35 and the switch server 31.

[0034] A buffer 34 is held until an exterior side switch (SW2) closes the demand

from an external network. Moreover, when it judges whether there are any inaccurate data in a demand from an external network and inaccurate data are detected, it has the function of filtering which cancels the demand.

[0035] The buffer 33 has the function to hold until an exterior side switch (SW2) closes the data by which the switch server 31 received the data from an internal network, and proper processing was carried out.

[0036] The seesaw switching box (SSWB) 35 consists of a bistable device (FF) and a switch (SW1, SW2), and controls one switch of the switches 1 or 2 by the value of the indication signal T from the switch tube system section 32 inputted into a bistable device (FF) in the short circuit condition.

[0037] That is, the seesaw switching box (SSWB) 35 receives the control signal from the switch tube system section 32, and it has the function which changes exclusively the switch by the side of the external network 2 and the internal network 1 (SW1 and SW2) by actuation of a flip-flop (FF). About this point, a truth table is shown in drawing 6 and the algorithm of a seesaw switching box (SSWB) of operation is explained to it.

[0038] Thus, at this example, each unit shown above can have a clear role respectively, and can protect important data from a cracking action or an unauthorized entry by having been independent and distributing. Since the switch tube system section 32 does not touch the data signal path on a network

at all especially, even if the crack of the switch server 31 or the buffers 33 and 34 is carried out, it can be perceived and a seesaw switching box (SSWB) can be controlled.

[0039] If the switch server 31 and buffers 33 and 34 are made into duplex structure using this control approach, the strengthening mold security system which changes automatically the unit by which cracking was carried out to a spare unit can be built.

[0040] In addition, the following patterns can be considered as timing to which the switch server 31 outputs operational mode change directions (timing chart of drawing 15) on the occasion of actual employment.

[0041] (1) The demand to a switch server changes to few time zones.

[0042] If a time zone with few demands is investigated based on the access situation to the switch server 31 and an external demand is not received to a switch server in the time zone, a user will be told and the communication link with an internal network will be performed between them.

(2) Change periodically.

[0043] When there is no time zone when a demand is disrupted, connection is changed from the exterior to the interior for every time amount specified beforehand. The time amount which the communication link with the interior of per time takes by increasing the count to change can be reduced, and delay of a

demand can be reduced from a user's external network.

(3) Change for every demand of a user.

[0044] For example, connection is changed at every inquiry of individual humanity news at the time of the application of wanting to see a certain specific individual's information among the individual humanity news accumulated in the internal network. Information can be kept by passing only necessary minimum information to an external network side. The above control of (1) thru/or (3) is performed based on the program installed in the storage of the switch server 1.

[0045] Next, actuation of this system is explained using drawing 7 thru/or drawing 10 .

[0046] In order to close either the switch by the side of the external network 2 (SW2), or the switch by the side of the internal network 1 (SW1) physically (structure which is not short-circuited), even if cracking of the switch control command or information reception-and-transmission server (here switch server 31) which controls switching of a SWSEC system even if is carried out, an internal network and an external network do not flow through the inside of this system (SWSEC) electrically.

[0047] Moreover, he stations each unit control (the switch server 31, the buffer 34, and buffer 33) and surveillance (here switch tube system section 32) which are not in contact with the data signal path on a network at all, and is trying not to

receive the control from the outside by cracking by performing switch control.

[0048] Here, also when a SWSEC system does not necessarily switch autonomously the timing which controls a switch 35, the switch server 31 issues a control command, and there is no demand from the external network 2, it can switch. When a demand is while being cut with the external network 2, the demand concerned is accumulated in a buffer 34 by switching and connection of a SWSEC system changes to the external network 2 side by it, the demand concerned is transmitted to the switch server 31 from a buffer 34.

[0049] When transmission of the switch server 31 and the external network 2 does not break off and continues, the time amount periodically connected to the internal network 1 is established, and the data which should be protected are transmitted to the internal network 1. The data which should be sent from the switch server 31 during transmission are stored in a buffer 33. Moreover, when there are many amounts of transmissions, the request to the information which does not need to be kept can always be received by preparing the information server (not shown) containing except the information which should be kept in an external network side.

[0050] Next, actuation is explained.

[0051] If there is a demand from the external network 2 side to the internal network 1, the demand signal will be accumulated in a buffer 34.

[0052] Here, it judges using the filter program for which what has an inaccurate demand, or a just thing was installed in the central processing unit (CPU) in a buffer 34 by external storage, and the demand will be canceled if inaccurate.

[0053] Next, if it is in packet buffer mode which shows the condition (condition that the internal network 1 and the switch server 31 are performing data communication) that the switch (SW2) of a seesaw switching box (SSWB) is cut (disconnection), a demand will be accumulated in a buffer 34. It stands by until it becomes the packet through mode which shows the condition (condition that the internal network 1 and the switch server 31 have ended data communication) that the switch (SW2) of a seesaw switching box (SSWB) is connected.

[0054] Termination of data communication of the internal network 1 and the switch server 31 sends out a control signal for the switch server 31 to change connection of the switch of the seesaw switching box (SSWB) 35 from a switch (SW1) to a switch (SW2) at the switch tube system section 32. The switch tube system section 32 which received this control signal sends out respectively the control signal for making into packet through mode whether the condition of a buffer 34 and a buffer 33 is packet buffer mode, or to be packet through mode, if it supervises and has become packet buffer mode to buffers 34 and 33. And if the control signal which shows the notice changed into packet buffer mode is respectively received from buffers 34 and 33, the control signal for changing

connection of a switch from SW1 to SW2 to a seesaw switching box (SSWB) is sent out. Moreover, if it is packet through mode, the control signal for changing connection of a switch from SW1 to SW2 is sent out to the seesaw switching box (SSWB) 35.

[0055] Said demand is inputted into the switch server 31 (switching control and information reception-and-transmission server) via the switch (SW2) and buffer 33 of a seesaw switching box (SSWB).

[0056] In the switch server 31, a central processing unit (CPU) judges proper and the purpose of a demand which were inputted above using a filter program, and if inaccurate, the demand will be canceled.

[0057] When a demand is proper, the control signal for changing connection of the switch of the seesaw switching box (SSWB) 35 from SW2 to SW1 is sent to the switch tube system section 32.

[0058] The switch tube system section 32 which received this control signal sends out respectively the control signal for making the condition of a buffer 34 and a buffer 33 into packet buffer mode to buffers 34 and 33. And if the control signal which shows the notice changed into packet buffer mode is respectively received from buffers 34 and 33, the control signal for changing connection of a switch from SW2 to SW1 to the seesaw switching box (SSWB) 35 is sent out.

[0059] Next, if the seesaw switching box (SSWB) 35 receives the control signal

sent from the switch tube system section 32, connection of a switch will be changed from SW2 to SW1 by actuation of a flip-flop (FF) (refer to drawing 8).

[0060] The switch server 31 sends out the demand suitable for the purpose to the internal network 1 side.

[0061] Next, the internal network 1 sends out data by the demand sent from the switch server 31, as shown in drawing 9 .

[0062] The data concerned are sent to the switch server 31 via the switch (SW1) of the short circuit condition of a seesaw switching box (SSWB).

[0063] The switch server 31 is formed in the proper format which suited for the purpose of the data. Based on the program installed in external storage, a central processing unit (CPU) performs this shaping.

[0064] Next, the switch server 31 sends out the data fabricated above by the buffer 33 which is packet buffer mode at the same time it sends the control signal for changing connection of the switch of a seesaw switching box (SSWB) from SW1 to SW2 to the switch tube system section 32.

[0065] The switch tube system section 32 which received the control signal from the switch server 31 sends out the control signal for changing connection of a switch from SW1 to SW2 to the seesaw switching box (SSWB) 35. Then, the control signal for making the condition of a buffer 33 into packet through mode is sent out to a buffer 33, and the control signal which shows the notice which

changed into packet through mode is received from a buffer 33.

[0066] Next, it is inputted into the buffer 34 with which data are packet buffer mode from the buffer 33 via the switch (SW2) of the seesaw switching box (SSWB) 35 as shown in drawing 10 .

[0067] A buffer 33 sends out the notice signal (buffer empty signal) to the switch tube system section 32, if it finishes transmitting data. The switch tube system section 32 which received the buffer empty signal sends out the control signal for making it packet through mode to the buffer 34 which is packet buffer mode.

[0068] The buffer 34 which received this control signal makes an own condition packet through mode, and answers the switch tube system section 32 in the control signal which shows the notice which changed into packet through mode.

[0069] Thus, data are transmitted to the external network 2. Next, the example of application of this example is explained using drawing 11 .

[0070] In this drawing, the case where it is required of the data server (internal network 1) installed in the company from the web server 1102 which has put the authentic act of Individual ID and a user attribute in Internet shopping on the provider, for example is assumed.

[0071] The external network 2 is connected to the Internet 21, and the Internet 21 concerned is connected to a provider's web server 1102 through the router 1101. This web server 1102 is connected to the Internet 22 through a router

1103, and the user terminal 1104 is connected to the Internet 22 concerned.

[0072] In the case of this drawing, actuation which outputs an authentication result as data from the internal network 1 based on the authentication demand from the external network 2 is performed, but this actuation is realized by above-mentioned drawing 7 thru/or explanation of drawing 10 .

[0073] Drawing 12 is a configuration in the case of the terminal unit 21 installed in domestic [individual] corresponding to an internal network, transmitting the download demand of musical piece data to the web server 1203 of the provider who is an external network, and receiving musical piece data from a web server 1203 to this.

[0074] In this drawing, through the router or the modular jack 21, the Internet 1201 is accessed and the Internet 1201 concerned is connected to a provider's web server 1203 via the router 1202. The musical piece data for music distributions are stored in the web server 1203.

[0075] In such music distribution service, transmission of musical piece data is required from a web server 1203 from the individual terminal unit 11. If attested by the approach which the demand concerned is received by the web server 1203, and this does not illustrate, musical piece data will be received by the control terminal 3 via a router and a modular jack 21 through the Internet 1201 from a web server 1203. About the procedure of reception of data, it is realizable

similarly by above-mentioned drawing 7 thru/or explanation of drawing 10 from dispatch of the demand at this time. However, in above-mentioned drawing 7 thru/or explanation of drawing 10 , it is necessary to read "a demand" as "data" and to read "data" as "a demand."

[0076] Moreover, it is possible to make this system intervene also in a data center enterprise, personal PC terminal, etc. in [LAN] a company and a provider besides the above example of application. That is, it is not limited to an above-mentioned example and its above-mentioned example of application, any parts on a network can be made to intervene, and this invention can maintain the internal security for every network.

[0077]

[Effect of the Invention] According to this invention, since it separates with the control signal of an access request [/ for the purpose of the external network and the internal network], an exchange of data is attained, without spoiling real time nature and bidirection.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the principle configuration of this invention (1)

[Drawing 2] The block diagram showing the principle configuration of this invention (2)

[Drawing 3] The block diagram showing the principle configuration of this invention (3)

[Drawing 4] The block diagram showing the principle configuration of this invention (4)

[Drawing 5] The detailed functional block diagram of an example

[Drawing 6] The configuration and table of truth value of a seesaw switching box (SSWB) of an example

[Drawing 7] The connection control unit actuation explanatory view of an example (1)

[Drawing 8] The connection control unit actuation explanatory view of an example (2)

[Drawing 9] The connection control unit actuation explanatory view of an example (3)

[Drawing 10] The connection control unit actuation explanatory view of an example (4)

[Drawing 11] The system chart showing the example of application of an example (1)

[Drawing 12] The system chart showing the example of application of an example (2)

[Drawing 13] The flow Fig. showing the shift procedure from the external communicate mode to the internal communicate mode in an example

[Drawing 14] The flow Fig. showing the shift procedure from the internal communicate mode to the external communicate mode in an example

[Drawing 15] The timing chart of the connection control device of an example

[Description of Notations]

1 Internal Network

2 External Network

21 Internet

22 Internet

3 Control Terminal (Control Unit)

31 Switch Server

32 Switch Tube System Section

33 Buffer (2nd Buffer)

34 Buffer (1st Buffer)

35 Seesaw Switching Box (SSWB)

1101 Router

1120 Web Server

1103 Router

1104 User Terminal

1201 Internet

1203 Web Server

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－7233
（P2002－7233A）
(43)公開日　平成14年１月11日(2002.1.11)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８９
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　11/20	Ｂ	５Ｋ０３０
12/22		11/26		

審査請求　未請求　請求項の数５　ＯＬ　（全 13 頁）

(21)出願番号　特願2000－182015(P2000－182015)

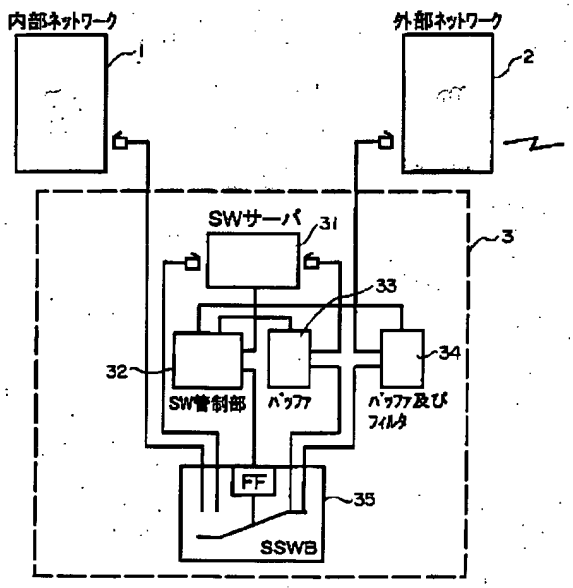
(22)出願日　平成12年６月16日(2000.6.16)

(71)出願人　500283088
株式会社　イオノス
東京都世田谷区宮坂１丁目36番18号
(72)発明者　星野　博一
東京都世田谷区宮坂１丁目36番18号　株式会社イオノス内
(74)代理人　100089244
弁理士　遠山　勉　（外１名）

Ｆターム(参考)　5B089 GA19 KA17 KB13 KC47 KD01
5K030 GA15 HA08 HC01 HC13 HD01
HD08 KA03

(54)【発明の名称】　通信路のスイッチ接続制御装置

(57)【要約】
【課題】　外部ネットワークからのアクセスに対し、物理的手段によって内部ネットワーク内への直接的な侵入を防ぎつつ、内部ネットワークと外部ネットワークとの柔軟な連携を可能とする。
【解決手段】　通信路に介在させ、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置とすることにより、目的別に分散した端末及びシステムに、シーソー式のスイッチング技術を用い不正侵入を防ぐセキュリティシステムを提供する。このようにシーソー式のスイッチング技術により、物理的に外部ネットワークと内部ネットワークとを目的に応じたアクセス要求の制御信号によって切り離すため、不正行為から確実にデータを守ることが可能となる。



【特許請求の範囲】
【請求項１】　通信路に介在され、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置。
【請求項２】　データの検証および制御を行う主制御装置と、
第１の通信路と接続された第１のバッファと、
前記主制御装置に接続され要求またはデータを蓄積する第２のバッファと、
前記第１のバッファと第２のバッファとを短絡・開放する第１のスイッチと、
前記主制御装置と第２の通信路とを短絡・開放する第２のスイッチと、
前記主制御装置からの指示により、前記第１または第２のいずれか一方のスイッチを排他的に短絡させるための制御信号を出力するスイッチ管制部とからなる通信路のスイッチ接続制御装置。
【請求項３】　前記第１のバッファは、第１の通信路からの要求またはデータの正当性を検証する検証手段を備えた請求項１記載の通信路のスイッチ接続制御装置。
【請求項４】　前記主制御装置は、第２の通信路からの要求またはデータの正当性を検証する検証手段を備えた請求項１記載の通信路のスイッチ接続制御装置。
【請求項５】　前記に加えて、主制御装置と第２のスイッチとの間に要求またはデータを蓄積する第３のバッファと、
前記第２の通信路と前記第２のスイッチとの間に要求またはデータを蓄積する第４のバッファとを備えた請求項２記載のスイッチ接続制御装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークにおけるセキュリティに適用して有効な技術に関する。
【０００２】
【従来の技術】インターネットの普及は、ビジネス形態を根本から変えるといわれている。
【０００３】データセンターやプロバイダー事業はおろかエンドユーザーまでが、インターネットに常時接続されている昨今、不正なアクセスによる犯罪が盛んになりつつある。いまやセキュリティの導入は政府機構から一個人までその必要性に迫られている。
【０００４】外部ネットワーク（インターネット等）から内部ネットワーク（イントラネット）へのアクセスを防止するためにファイアウォール技術が知られている。
【０００５】このような従来技術のセキュリティは、すべての端末及びシステムが物理上あるいは論理上一本のラインでつながっており、ファイアウォールにより論理的に適正を判断していた。
【０００６】
【発明が解決しようとする課題】従来のネットワークセキュリティ技術では、すべての端末及びシステムが物理上あるいは論理上一本のラインでつながっているため、不正な侵入が可能であるという問題点を抱えている。
【０００７】このためには、外部ネットワークと内部ネットワークとを切り離すことが最も安全である。すなわち、どのような事態（破壊攻撃等）においても一本のラインでつながることがないため、不正な侵入を防御できる。
【０００８】ところが、外部ネットワークから内部ネットワークに対してのアクセス、あるいは内部ネットワークから外部ネットワークへのアクセスが完全に遮断されてしまうと、ネットワーク相互の柔軟な運用が不可能となってしまう。
【０００９】つまり、外部ネットワークと内部ネットワークとを物理的に切り離すことはリアルタイム性や双方向性が損なわれる恐れがある。
【００１０】本発明は、外部ネットワークからのアクセスに対し、物理的手段によって内部ネットワーク内への直接的な侵入を防ぎつつ、内部ネットワークと外部ネットワークとの柔軟な連携を可能とすることを技術的課題とする。
【００１１】
【課題を解決するための手段】本発明は、通信路に介在され、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置である。
【００１２】すなわち、目的別に分散した端末及びシステムに、シーソー式のスイッチング技術を用い不正侵入を防ぐセキュリティシステムを提供する。
【００１３】シーソー式のスイッチング技術により、物理的に外部ネットワークと内部ネットワークとを目的に応じたアクセス要求の制御信号によって切り離すため、不正行為から確実にデータを守ることが可能となる。
【００１４】
【発明の実施の形態】
【００１５】
【実施例】以下、図面に基づいて、本発明の実施の形態を説明する。
【００１６】図１は、本発明の概念を示す機能ブロック図である。
【００１７】図1に示すように、目的別の端末及びシステムを以下の３つに分類・分散する。
【００１８】同図中、１は、重要なデータやシステムを保有する内部ネットワークであり、コンピュータシステムを通信回線で接続した汎用のネットワークで構成されている。ここで、内部ネットワークとは、上記に示す有線あるいは無線を含めた外線と繋がっていない端末あるいはネットワークを有するシステムを内部ネットワークという。図中２は外部ネットワークである。ここで外部ネットワークとは、インターネット網あるいは公衆網あ

るいは専用線等の有線あるいは無線を含めた外線と繋がっているネットワークあるいはネットワークを有するシステムあるいは端末あるいはモジュラージャック等のネットワーク構成部品を外部ネットワークという。３は、本発明の最も重要な要素となる、内部ネットワークと外部ネットワークとを制御するための制御端末（シーソー式スイッチングセキュリティシステム）である。

【００１９】制御端末３は、さらに、スイッチサーバ３１、スイッチ管制部３２、バッファ３３、バッファ３４およびシーソースイッチングボックス（ＳＳＷＢ）３５とで構成されている。これらの各機能部については後で詳述する。

【００２０】このシステムにおいて、制御端末３は、図２に示すように、外部ネットワークからの要求を受信し、内部ネットワークへ送信する機能を有している。また、内部ネットワークのデータを受信し、外部ネットワークへ送信する機能を有している。同図において、シーソースイッチングボックス（ＳＳＷＢ）５は、外部ネットワーク２からの要求信号を内部ネットワーク１に伝えるために、バッファ３４をバッファ３３と接続した状態となっている。

【００２１】また、制御端末３は、図３に示すように、内部ネットワークからの要求を受信し、外部ネットワークへ送信する機能を有している。また、外部ネットワークのデータを受信し、内部ネットワークへ送信する機能を有している。同図において、シーソースイッチングボックス（ＳＳＷＢ）５は、内部ネットワーク１からの要求信号を外部ネットワーク２に伝えるために、内部ネットワーク１とスイッチサーバ３１とを接続した状態となっている。

【００２２】制御端末３はまた、図４に示すように、内部ネットワーク１または外部ネットワーク２の双方において、要求信号、データ信号を双方向に送受信することも可能である。

【００２３】このような双方向のモードで使用する場合には、スイッチサーバ３１とシーソースイッチングボックス（ＳＳＷＢ）３５との間にバッファ３７を介装し、さらに内部ネットワーク１とシーソースイッチングボックス（ＳＳＷＢ）３５との間にもバッファ３６を介装して、制御端末３内が内部ネットワーク１、外部ネットワーク２に対して左右対称構成となるようにしてもよい。この場合、バッファ３６は、内部ネットワークからの要求を外部側スイッチ（ＳＷ２）が閉じるまで、保持する。また、内部ネットワークからの要求に不正なデータがないかを判断し、不正データが検出されるとその要求を破棄するフィルタリングの機能を有する。

【００２４】バッファ３７は、外部ネットワーク２からのデータをスイッチサーバ３１が受け、適正処理されたデータを内部側スイッチ（ＳＷ２）が閉じるまで、保持する機能を有している。

【００２５】その他の制御端末３の動作については、前述の図２乃至３で説明したものと同様であるので説明は省略する。

【００２６】なお、制御端末３内を左右対称構造としたものは図４だけで示したが、このような構造は制御端末３をいずれのモードで使用した場合にも適用可能である。

【００２７】次に、図５を用いて、本実施例のオブジェクト分散型ユニット（目的別によって分散されたユニット）における各ユニットの構成、機能及びその動作を説明する。

【００２８】スイッチサーバ３１は、コンピュータシステムにより構成されており、バスを中心に中央処理装置（ＣＰＵ）、メモリ、外部記憶装置、インターフェース（Ｉ／Ｏ）等で構成されている。外部記憶装置にはプログラムがインストールされており、中央処理装置（ＣＰＵ）は当該プログラムをメモリにロードして順次実行することによって、スイッチ管制部３２に対してシーソースイッチングボックス（ＳＳＷＢ）３５の制御指示信号を出力するようになっている。

【００２９】つまり、スイッチサーバ３１は、外部ネットワークからの要求により、内部ネットワークへ必要なデータを要求したり、内部ネットワークから受け取ったデータと外部ネットワークからの要求の整合性を図る等、目的に応じた処理を行う。また、要求やデータ等の信号を元に外部ネットワーク側と内部ネットワーク側のそれぞれのゲート（ＳＷ１及びＳＷ２）を排他的に切り替える為の制御信号をスイッチ管制部３２に送る。

【００３０】スイッチ管制部３２は、中央処理装置（ＣＰＵ）およびメモリを中心に複数のインターフェース（Ｉ／Ｏ）で構成されている。すなわち、スイッチサーバ３１からの制御指示信号に基づいてシーソースイッチングボックス（ＳＳＷＢ）３５を制御するようになっている。

【００３１】ここで、スイッチ管制部３２は、ネットワーク上のデータ信号経路にまったく接触しておらず、スイッチサーバ３１、バッファ３４、バッファ３３、シーソースイッチングボックス（ＳＳＷＢ）をそれぞれ監視することで、ユニットの状態を管理する役割を有している。

【００３２】そして、バッファ３４、バッファ３３に対しては、スイッチサーバ３１等からの情報を元に各々のモード変更の制御信号を送る。（図１３乃至１４を参照）また、スイッチサーバ３１に対しては、上記のバッファ３４，３３のモード状態信号を送る。また、スイッチサーバ３１からシーソースイッチングボックス（ＳＳＷＢ）３５へのスイッチ切り替え制御信号を受け、バッファ３４，３３のモード状態との適正を判断し、シーソースイッチングボックス（ＳＳＷＢ）に対してスイッチ切り替え制御信号を送る機能を有している。

【００３３】バッファ３３および３４はほぼ同様の構成を有しているが、バッファ３４は外部ネットワークに直接接続されている点、バッファ３３はシーソースイッチングボックス（ＳＳＷＢ）３５とスイッチサーバ３１との間に介装されている点が異なる。

【００３４】バッファ３４は、外部ネットワークからの要求を外部側スイッチ（ＳＷ２）が閉じるまで、保持する。また、外部ネットワークからの要求に不正なデータがないかを判断し、不正データが検出されるとその要求を破棄するフィルタリングの機能を有する。

【００３５】バッファ３３は、内部ネットワークからのデータをスイッチサーバ３１が受け、適正処理されたデータを外部側スイッチ（ＳＷ２）が閉じるまで、保持する機能を有している。

【００３６】シーソースイッチングボックス（ＳＳＷＢ）３５は、フリップフロップ素子（ＦＦ）と、スイッチ（ＳＷ１，ＳＷ２）とで構成されており、フリップフロップ素子（ＦＦ）に入力されるスイッチ管制部３２からの指示信号Ｔの値によって、スイッチ１または２のいずれかのスイッチを短絡状態に制御するようになっている。

【００３７】つまり、シーソースイッチングボックス（ＳＳＷＢ）３５は、スイッチ管制部３２からの制御信号を受け、フリップフロップ（ＦＦ）の動作により、外部ネットワーク２側と内部ネットワーク１側のスイッチ（ＳＷ１及びＳＷ２）を排他的に切り替える機能を有している。この点については、図６に真理値表を示してシーソースイッチングボックス（ＳＳＷＢ）の動作アルゴリズムを説明している。

【００３８】このように、本実施例では、上記に示す各ユニットが、各々明確な役割を持ち、独立・分散していることで、クラッキング行為や不正侵入から大切なデータを守ることができる。特に、スイッチ管制部３２がネットワーク上のデータ信号経路にまったく接触していないため、スイッチサーバ３１やバッファ３３，３４がクラックされたとしても、それを察知し、シーソースイッチングボックス（ＳＳＷＢ）を制御することができる。

【００３９】この制御方法を利用して、スイッチサーバ３１やバッファ３３，３４をデュープレックス構造にすれば、クラッキングされたユニットを予備のユニットに自動的に切り替える強化型セキュリティシステムを構築できる。

【００４０】なお、実際の運用に際してスイッチサーバ３１が運用モード切替指示（図１５のタイミングチャート）を出力するタイミングとしては、以下のようなパターンが考えられる。

【００４１】（１）スイッチサーバへの要求が少ない時間帯に切り替える。

【００４２】スイッチサーバ３１へのアクセス状況を基に要求の少ない時間帯を調べ、その時間帯にスイッチサーバへ外部の要求を受け付けられないと、ユーザーには知らせ、その間に内部ネットワークとの通信を行う。

（２）定期的に切り替える。

【００４３】要求のとぎれる時間帯がない場合、あらかじめ指定した時間ごとに接続を外部から内部へ切り替える。切り替える回数を増やすことで１回あたりの内部との通信にかかる時間を減らして、ユーザーの外部ネットワークから要求の遅延を減らすことができる。

（３）ユーザーの要求ごとに切り替える。

【００４４】例えば、内部ネットワークに蓄積している個人情報のうち、ある特定個人の情報を見たい、というアプリケーションの時に、個人情報の問い合わせの都度接続を切り替える。必要最低限の情報のみを外部ネットワーク側へ流すことで、情報を守ることができる。以上のような（１）乃至（３）の制御は、スイッチサーバ１の記憶装置にインストールされたプログラムに基づいて行われる。

【００４５】次に、図７乃至図１０を用いて、本システムの動作を説明する。

【００４６】本システム（ＳＷＳＥＣ）内は、物理的に外部ネットワーク２側のスイッチ（ＳＷ２）または内部ネットワーク１側のスイッチ（ＳＷ１）のいずれか一方しか閉じない（短絡しない構造の）ため、たとえＳＷＳＥＣシステムのスイッチングを制御するスイッチ制御指令または情報受発信サーバ（ここではスイッチサーバ３１）がクラッキングされても、内部ネットワークと外部ネットワークが電気的に導通することはない。

【００４７】また、ネットワーク上のデータ信号経路にまったく接触していない各ユニット（スイッチサーバ３１、バッファ３４、バッファ３３の）制御及び監視機構（ここではスイッチ管制部３２）を配置し、スイッチ制御を行うことでクラッキングによる外部からの制御を受付けないようにしている。

【００４８】ここでは、スイッチ３５を制御するタイミングを、ＳＷＳＥＣシステムが自律的にスイッチングする訳ではなく、スイッチサーバ３１が制御指令を出すことにより、外部ネットワーク２から要求の無いときにもスイッチングを行うことができる。スイッチングによって、外部ネットワーク２と切断されている間に要求があった場合は、バッファ３４に当該要求が蓄積され、ＳＷＳＥＣシステムの接続が外部ネットワーク２側に切り替わった際に当該要求がバッファ３４からスイッチサーバ３１に伝送される。

【００４９】スイッチサーバ３１と外部ネットワーク２の伝送が途切れなく続く場合は、定期的に内部ネットワーク１に接続する時間を設け、守るべきデータを内部ネットワーク１に伝送する。伝送中にスイッチサーバ３１から発信すべきデータは、バッファ３３に蓄積される。また、伝送量が多い場合は、守るべき情報以外がはいっている情報サーバ（図示せず）を外部ネットワーク側に

設けることで、守らなくてよい情報に対するリクエストを常時受け付けることができる。

【００５０】次に動作を説明する。

【００５１】外部ネットワーク２側から内部ネットワーク１に対して要求があるとその要求信号は、バッファ３４に蓄積される。

【００５２】ここで、要求が不正なものか正当なものかをバッファ３４内の中央処理装置（ＣＰＵ）が外部記憶装置にインストールされたフィルタプログラムを用いて判断し、不正なものであればその要求を破棄する。

【００５３】次に、シーソースイッチングボックス（ＳＳＷＢ）のスイッチ（ＳＷ２）が切断（開放）されている状態（内部ネットワーク１とスイッチサーバ３１とがデータ通信を行っている状態）を示すパケットバッファモードであれば、要求はバッファ３４に蓄積され、シーソースイッチングボックス（ＳＳＷＢ）のスイッチ（ＳＷ２）が接続される状態（内部ネットワーク１とスイッチサーバ３１がデータ通信を終了している状態）を示すパケットスルーモードになるまで待機する。

【００５４】内部ネットワーク１とスイッチサーバ３１がデータ通信を終了するとスイッチサーバ３１がスイッチ管制部３２にシーソースイッチングボックス（ＳＳＷＢ）３５のスイッチの接続をスイッチ（ＳＷ１）からスイッチ（ＳＷ２）に切り替えるための制御信号を送出する。この制御信号を受け取ったスイッチ管制部３２は、バッファ３４及びバッファ３３の状態がパケットバッファモードになっているかパケットスルーモードになっているかを監視し、パケットバッファモードになっていれば、パケットスルーモードにするための制御信号を各々バッファ３４、３３に送出する。そして、パケットバッファモードに変更した通知を示す制御信号を各々バッファ３４，３３から受け取ると、シーソースイッチングボックス（ＳＳＷＢ）に対してスイッチの接続をＳＷ１からＳＷ２に切り替えるための制御信号を送出する。また、パケットスルーモードになっていれば、シーソースイッチングボックス（ＳＳＷＢ）３５にスイッチの接続をＳＷ１からＳＷ２に切り替えるための制御信号を送出する。

【００５５】前記要求は、シーソースイッチングボックス（ＳＳＷＢ）のスイッチ（ＳＷ２）及びバッファ３３を経由して、スイッチサーバ３１（スイッチング制御及び情報受発信サーバ）に入力される。

【００５６】スイッチサーバ３１では、前記で入力された要求の適正及び目的を、中央処理装置（ＣＰＵ）がフィルタプログラムを用いて判断し、不正なものであればその要求を破棄する。

【００５７】要求が適正である場合には、シーソースイッチングボックス（ＳＳＷＢ）３５のスイッチの接続をＳＷ２からＳＷ１に切り替えるための制御信号をスイッチ管制部３２に送る。

【００５８】この制御信号を受信したスイッチ管制部３２は、バッファ３４及びバッファ３３の状態をパケットバッファモードにするための制御信号を各々バッファ３４、３３に送出する。そして、パケットバッファモードに変更した通知を示す制御信号を各々バッファ３４，３３から受け取ると、シーソースイッチングボックス（ＳＳＷＢ）３５に対してスイッチの接続をＳＷ２からＳＷ１に切り替えるための制御信号を送出する。

【００５９】次に、スイッチ管制部３２から送られてきた制御信号をシーソースイッチングボックス（ＳＳＷＢ）３５が受け取るとフリップフロップ（ＦＦ）の動作により、スイッチの接続をＳＷ２からＳＷ１に切り替える（図８参照）。

【００６０】スイッチサーバ３１は、内部ネットワーク１側に目的に合った要求を送出する。

【００６１】次に、内部ネットワーク１は、図９に示すように、スイッチサーバ３１より送られてきた要求により、データを送出する。

【００６２】当該データは、シーソースイッチングボックス（ＳＳＷＢ）の短絡状態のスイッチ（ＳＷ１）を経由して、スイッチサーバ３１に送られる。

【００６３】スイッチサーバ３１は、そのデータを目的に合った適正な形式に形成する。この成形は外部記憶装置にインストールされたプログラムに基づいて中央処理装置（ＣＰＵ）が行う。

【００６４】次に、スイッチサーバ３１は、シーソースイッチングボックス（ＳＳＷＢ）のスイッチの接続をＳＷ１からＳＷ２に切り替えるための制御信号をスイッチ管制部３２に送ると同時に、パケットバッファモードになっているバッファ３３に前記で成形されたデータを送出する。

【００６５】スイッチサーバ３１からの制御信号を受け取ったスイッチ管制部３２は、シーソースイッチングボックス（ＳＳＷＢ）３５にスイッチの接続をＳＷ１からＳＷ２に切り替えるための制御信号を送出する。続いて、バッファ３３の状態をパケットスルーモードにするための制御信号をバッファ３３に送出し、パケットスルーモードに変更した通知を示す制御信号をバッファ３３から受け取る。

【００６６】次に、図１０に示すように、データがバッファ３３からシーソースイッチングボックス（ＳＳＷＢ）３５のスイッチ（ＳＷ２）を経由して、パケットバッファモードになっているバッファ３４に入力される。

【００６７】バッファ３３は、データを送信し終わるとその通知信号（バッファエンプティ信号）をスイッチ管制部３２に送出する。バッファエンプティ信号を受け取ったスイッチ管制部３２は、パケットバッファモードになっているバッファ３４に対してパケットスルーモードにするための制御信号を送出する。

【００６８】この制御信号を受け取ったバッファ３４

は、自身の状態をパケットスルーモードにし、パケットスルーモードに変更した通知を示す制御信号をスイッチ管制部３２に返信する。

【００６９】このようにしてデータが外部ネットワーク２に伝送される。次に、本実施例の適用例を図１１を用いて説明する。

【００７０】同図では、たとえば、インターネットショッピングにおける個人ＩＤとユーザー属性の認証行為をプロバイダに置いているウェブサーバ１１０２から企業内に設置されたデータサーバ（内部ネットワーク１）へ要求された場合を想定している。

【００７１】外部ネットワーク２は、インターネット２１に接続されており、当該インターネット２１は、ルータ１１０１を介してプロバイダのウェブサーバ１１０２に接続されている。このウェブサーバ１１０２は、ルータ１１０３を介してインターネット２２に接続され、当該インターネット２２にはユーザ端末１１０４が接続されている。

【００７２】同図の場合、外部ネットワーク２からの認証要求に基づいて内部ネットワーク１から認証結果をデータとして出力する動作を行うが、この動作は前述の図７乃至図１０の説明で実現される。

【００７３】図１２は、個人の家庭内に設置された端末装置２１が内部ネットワークに該当し、外部ネットワークであるプロバイダのウェブサーバ１２０３に対して楽曲データのダウンロード要求を送信し、これに対してウェブサーバ１２０３から楽曲データを受信する場合の構成である。

【００７４】同図において、ルータやモジュラージャック２１を介して、インターネット１２０１に接続されており、当該インターネット１２０１は、ルータ１２０２を経由してプロバイダのウェブサーバ１２０３に接続されている。ウェブサーバ１２０３には音楽配信用の楽曲データが蓄積されている。

【００７５】このような音楽配信サービスにおいて、個人の端末装置１１からウェブサーバ１２０３に対して楽曲データの送信を要求する。当該要求がウェブサーバ１２０３で受信されこれが図示しない方法で認証されると、ウェブサーバ１２０３から楽曲データがインターネット１２０１を介してルータ及びモジュラージャック２１を経由して制御端末３に受信される。このときの要求の発信からデータの受信の手順については、前述の図７乃至図１０の説明で同様に実現することができる。ただし、前述の図７乃至図１０の説明において、「要求」を「データ」、「データ」を「要求」と読み替える必要がある。

【００７６】また、以上の適用例以外にも、企業内ＬＡＮやプロバイダー内、データセンター事業、個人用ＰＣ端末などにおいても本システムを介在させることが可能である。すなわち、本発明は、前述の実施例およびその適用例に限定されるものではなく、ネットワーク上の如何なる部分にも介在させることができ、ネットワーク毎の内部セキュリティを維持することが可能である。

【００７７】

【発明の効果】本発明によれば、外部ネットワークと内部ネットワークとを目的に応じたアクセス要求の制御信号によって切り離すため、リアルタイム性や双方向性が損なわれることなくデータのやり取りが可能となる。

【図面の簡単な説明】

【図１】　本発明の原理構成を示すブロック図（１）

【図２】　本発明の原理構成を示すブロック図（２）

【図３】　本発明の原理構成を示すブロック図（３）

【図４】　本発明の原理構成を示すブロック図（４）

【図５】　実施例の詳細な機能ブロック図

【図６】　実施例のシーソースイッチングボックス（ＳＳＷＢ）の構成および真理値表

【図７】　実施例の接続制御装置動作説明図（１）

【図８】　実施例の接続制御装置動作説明図（２）

【図９】　実施例の接続制御装置動作説明図（３）

【図１０】　実施例の接続制御装置動作説明図（４）

【図１１】　実施例の適用例を示すシステム図（１）

【図１２】　実施例の適用例を示すシステム図（２）

【図１３】　実施例において外部通信モードから内部通信モードへの移行手順を示すフロー図

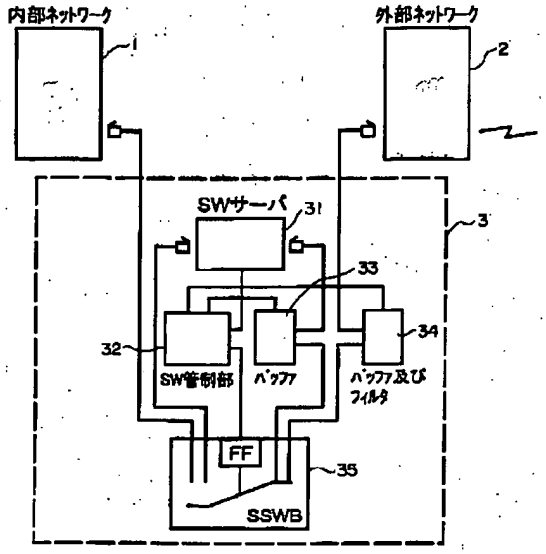
【図１４】　実施例において内部通信モードから外部通信モードへの移行手順を示すフロー図

【図１５】　実施例の接続制御装置のタイミングチャート

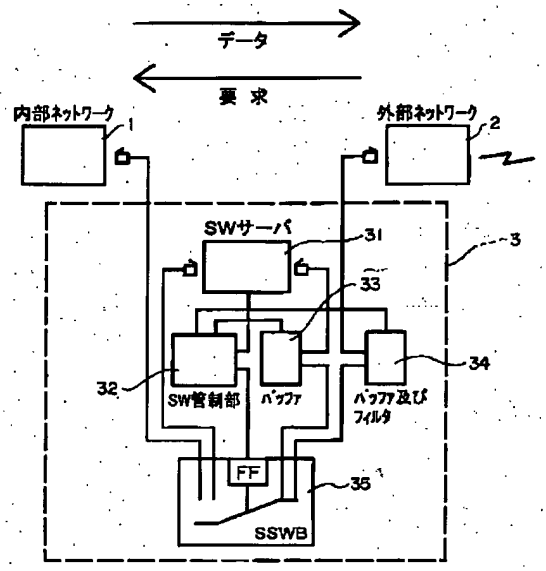
【符号の説明】

１　内部ネットワーク
２　外部ネットワーク
２１　インターネット
２２　インターネット
３　制御端末（制御装置）
３１　スイッチサーバ
３２　スイッチ管制部
３３　バッファ（第２バッファ）
３４　バッファ（第１バッファ）
３５　シーソースイッチングボックス（ＳＳＷＢ）
１１０１　ルータ
１１２０　ウェブサーバ
１１０３　ルータ
１１０４　ユーザ端末
１２０１　インターネット
１２０３　ウェブサーバ

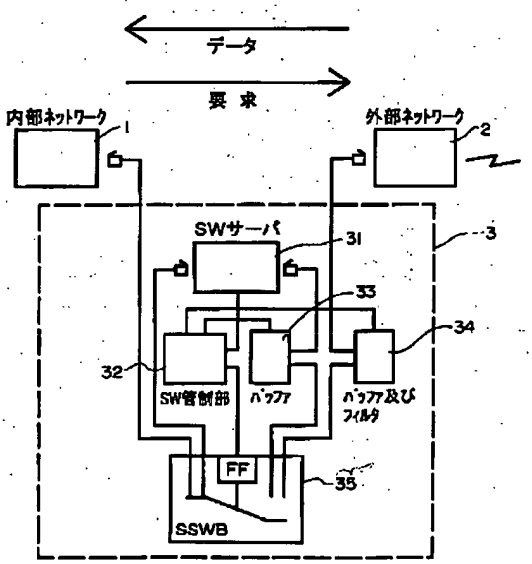
【図１】


内部ネットワーク
1
外部ネットワーク
2
SWサーバ
31
3
33
32
34
SW管制部
バッファ
バッファ及び
フィルタ
FF
35
SSWB

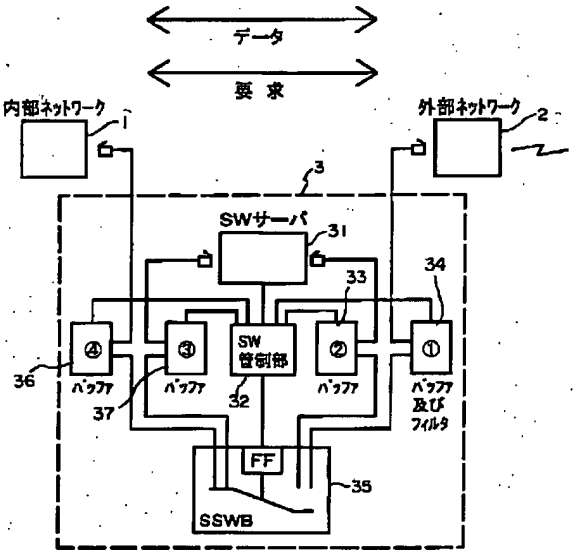
【図２】


データ
要求
内部ネットワーク
1
外部ネットワーク
2
SWサーバ
31
3
33
32
34
SW管制部
バッファ
バッファ及び
フィルタ
FF
35
SSWB

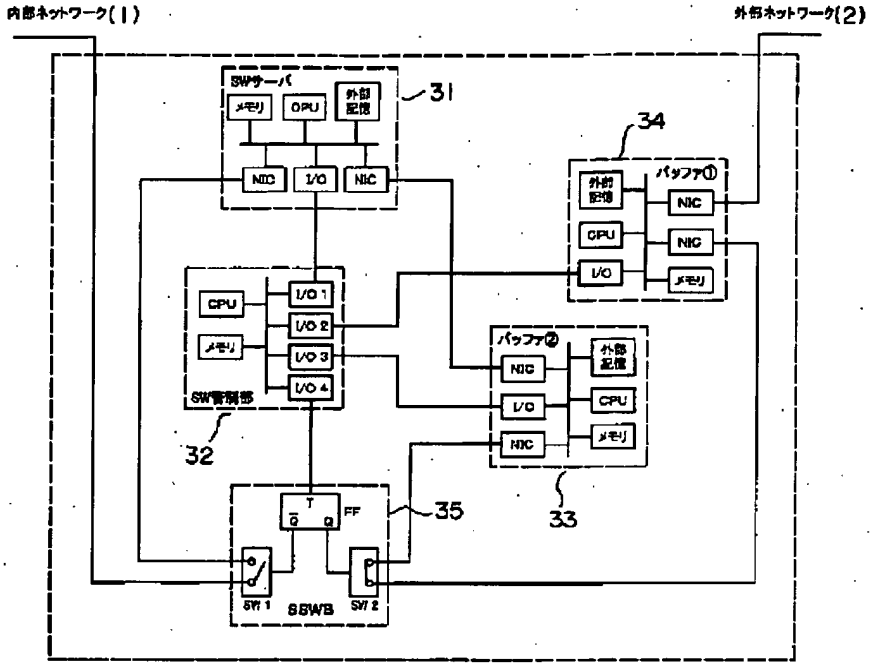
【図３】


データ
要求
内部ネットワーク
1
外部ネットワーク
2
SWサーバ
31
3
33
32
34
SW管制部
バッファ
バッファ及び
フィルタ
FF
35
SSWB

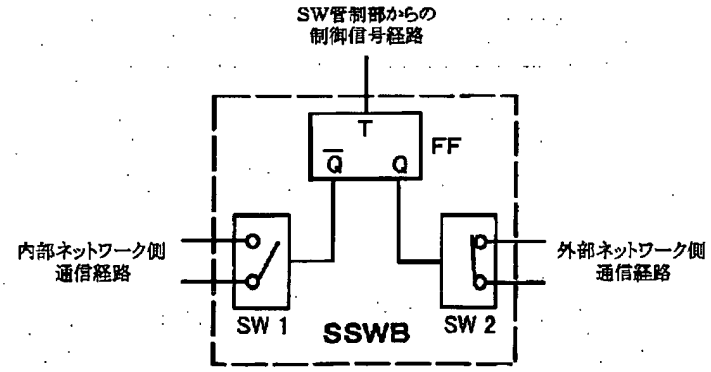
【図４】


データ
要求
内部ネットワーク
1
外部ネットワーク
2
3
SWサーバ
31
33
34
④
③
SW
管制部
②
①
36
バッファ
37
バッファ
32
バッファ
バッファ
及び
フィルタ
FF
35
SSWB

【図５】



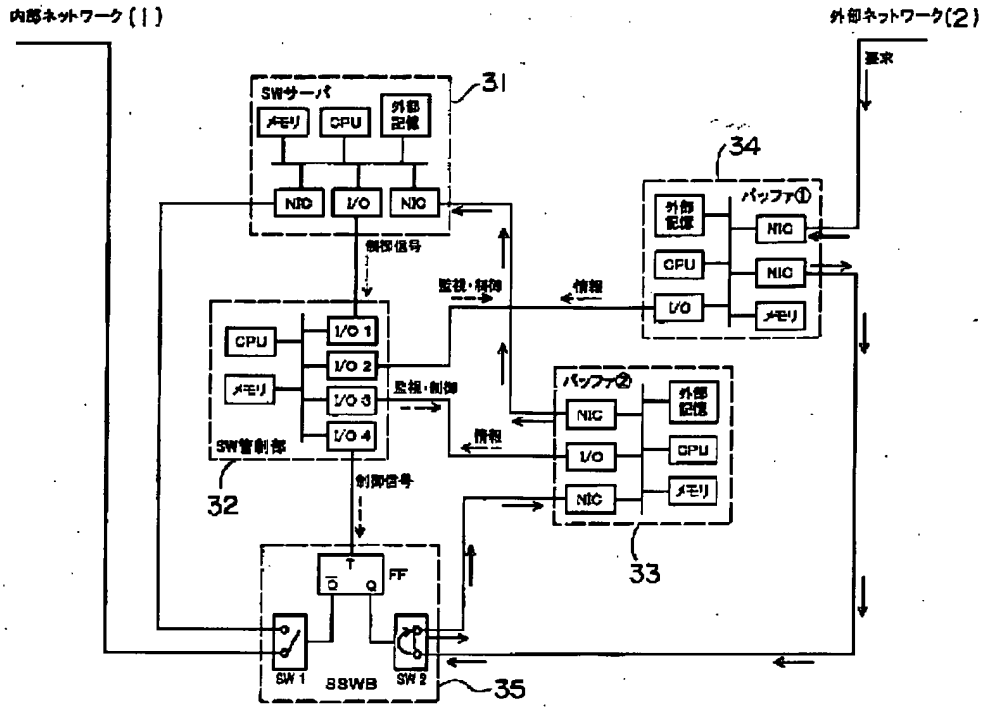
【図６】



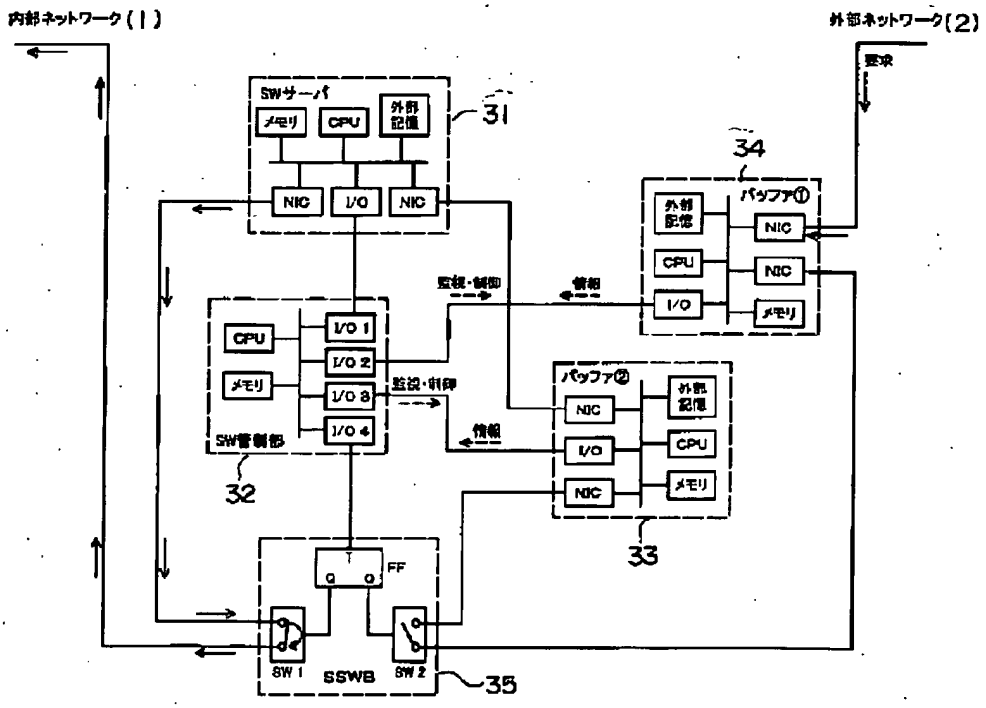
＜ＳＷ１とＳＷ２を制御するカットフリップフロップの真理値表＞

T	Q　　$\overline{Q}$
0	変化しない
1	反転する

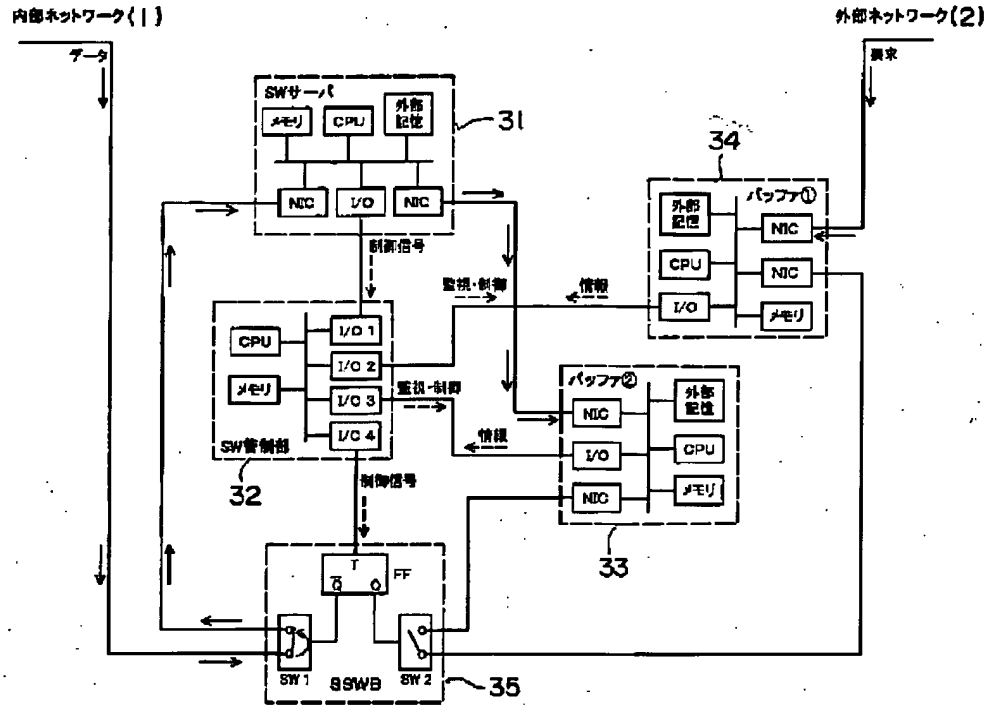
【図７】


内部ネットワーク(1)
外部ネットワーク(2)
要求
SWサーバ
メモリ
CPU
外部記憶
NIC
I/O
31
34
バッファ①
監視信号
監視・制御
情報
CPU
メモリ
I/O 1
I/O 2
I/O 3
I/O 4
SW管制部
32
制御信号
バッファ②
33
FF
SW 1
SSWB
SW 2
35

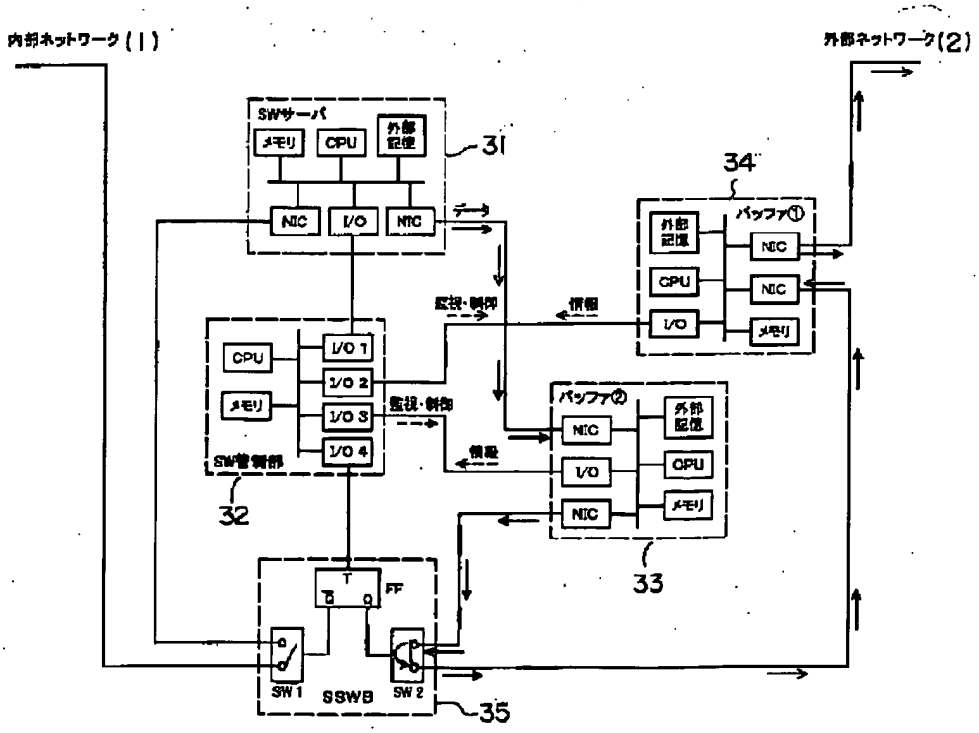
【図８】


内部ネットワーク(1)
外部ネットワーク(2)
要求
SWサーバ
メモリ
CPU
外部記憶
NIC
I/O
31
34
バッファ①
監視・制御
情報
CPU
メモリ
I/O 1
I/O 2
I/O 3
I/O 4
SW管制部
32
バッファ②
33
FF
SW 1
SSWB
SW 2
35

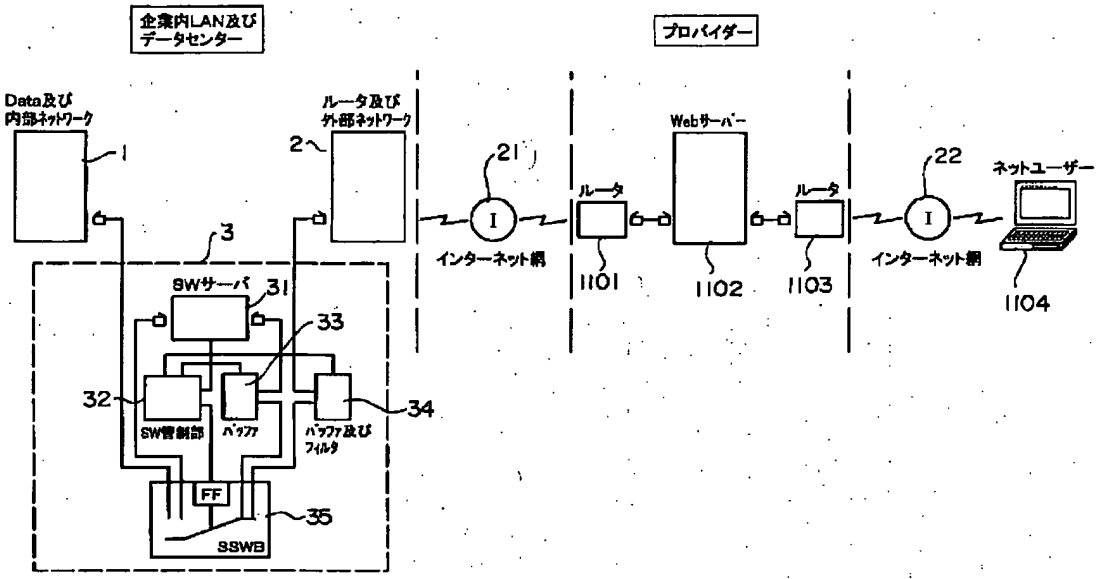
【図９】


内部ネットワーク(1)
外部ネットワーク(2)
データ
要求
SWサーバ
メモリ
CPU
外部記憶
NIC
I/O
31
34
バッファ①
制御信号
監視・制御
情報
CPU
I/O 1
I/O 2
I/O 3
I/O 4
メモリ
SW管制部
32
バッファ②
制御信号
FF
SW 1
SSWB
SW 2
35
33

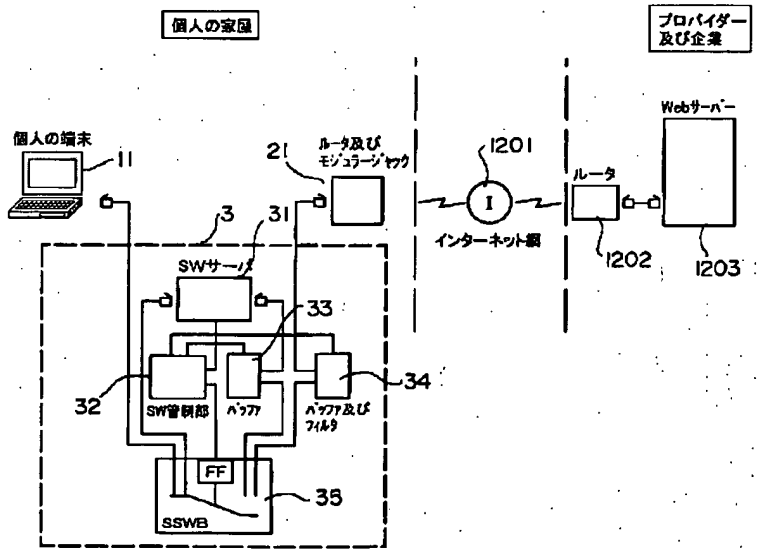
【図１０】


内部ネットワーク(1)
外部ネットワーク(2)
SWサーバ
メモリ
CPU
外部記憶
NIC
I/O
31
34
バッファ①
データ
監視・制御
情報
CPU
I/O 1
I/O 2
I/O 3
I/O 4
メモリ
SW管制部
32
バッファ②
FF
SW 1
SSWB
SW 2
35
33

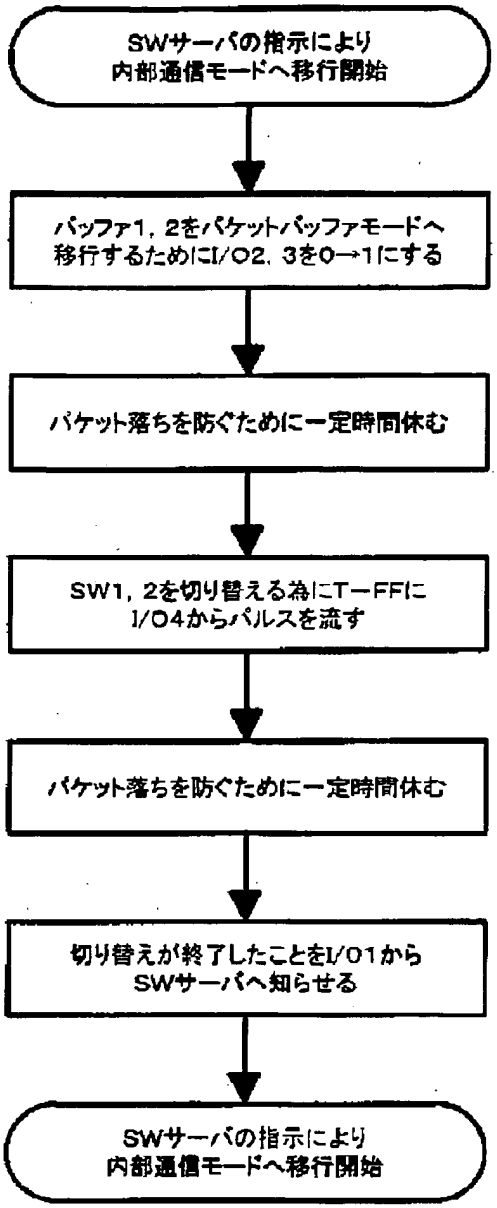
【図１１】


企業内LAN及び
データセンター
プロバイダー
Data及び
内部ネットワーク
ルータ及び
外部ネットワーク
Webサーバー
ルータ
ルータ
ネットユーザー
1
2
21
22
3
SWサーバ
31
33
32
34
SW管制部
バッファ
バッファ及び
フィルタ
FF
35
SSWB
インターネット網
インターネット網
1101
1102
1103
1104

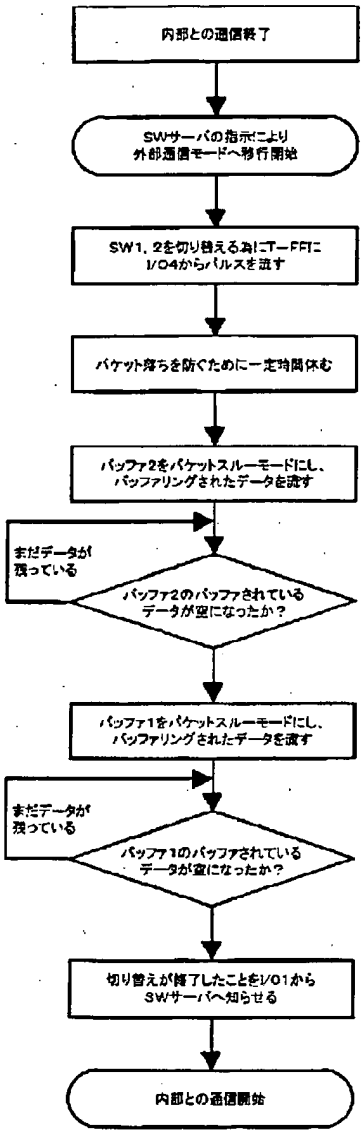
【図１２】


個人の家庭
プロバイダー
及び企業
個人の端末
ルータ及び
モジュラージャック
Webサーバー
11
21
1201
3
31
ルータ
SWサーバ
33
32
34
SW管制部
バッファ
バッファ及び
フィルタ
FF
35
SSWB
インターネット網
1202
1203

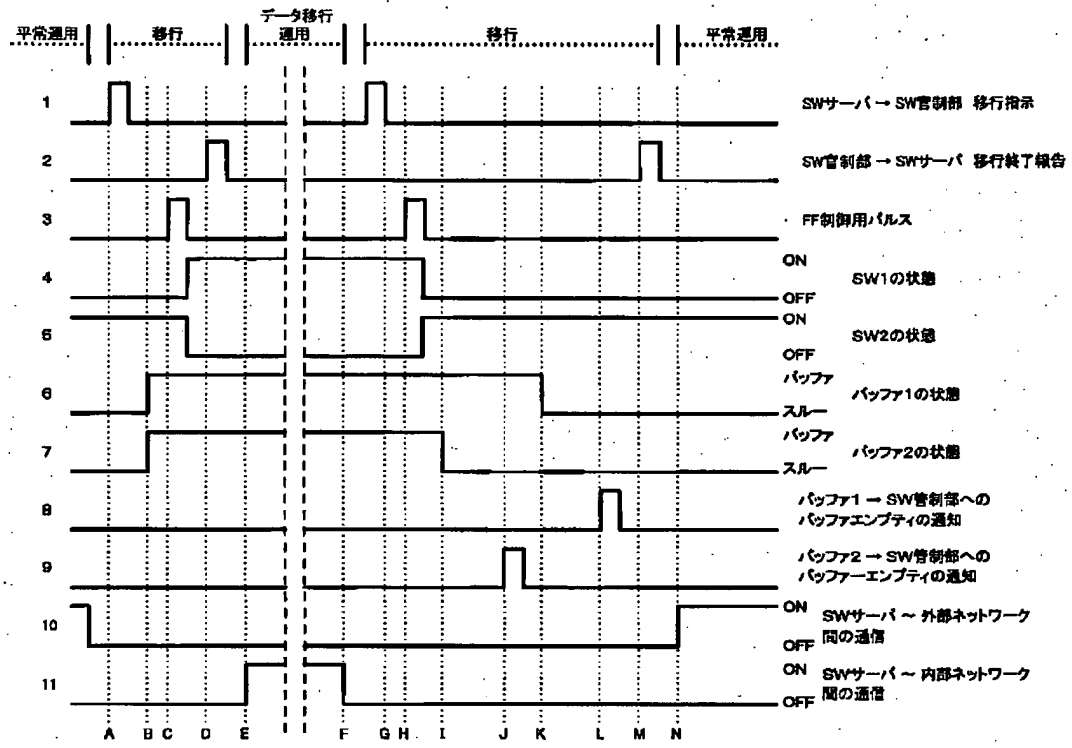
【図１３】


SWサーバの指示により
内部通信モードへ移行開始
バッファ1，2をパケットバッファモードへ
移行するためにI/O2，3を0→1にする
パケット落ちを防ぐために一定時間休む
SW1，2を切り替える為にT－FFに
I/O4からパルスを流す
パケット落ちを防ぐために一定時間休む
切り替えが終了したことをI/O1から
SWサーバへ知らせる
SWサーバの指示により
内部通信モードへ移行開始

【図１４】


内部との通信終了
SWサーバの指示により
外部通信モードへ移行開始
SW1，2を切り替える為にT－FFに
I/O4からパルスを流す
パケット落ちを防ぐために一定時間休む
バッファ2をパケットスルーモードにし、
バッファリングされたデータを流す
まだデータが
残っている
バッファ2のバッファされている
データが空になったか？
バッファ1をパケットスルーモードにし、
バッファリングされたデータを流す
まだデータが
残っている
バッファ1のバッファされている
データが空になったか？
切り替えが終了したことをI/O1から
SWサーバへ知らせる
内部との通信開始

【図１５】


平常運用
移行
データ移行
運用
移行
平常運用
1
2
3
4
5
6
7
8
9
10
11
SWサーバ→SW管制部 移行指示
SW管制部→SWサーバ 移行終了報告
FF制御用パルス
ON
OFF
SW1の状態
ON
OFF
SW2の状態
バッファ
スルー
バッファ1の状態
バッファ
スルー
バッファ2の状態
バッファ1→SW管制部への
バッファエンプティの通知
バッファ2→SW管制部への
バッファーエンプティの通知
ON
OFF
SWサーバ～外部ネットワーク
間の通信
ON
OFF
SWサーバ～内部ネットワーク
間の通信
A
B
C
D
E
F
G
H
I
J
K
L
M
N

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成１９年６月２１日（２００７．６．２１）

【公開番号】特開２００２－７２３３（Ｐ２００２－７２３３Ａ）
【公開日】平成１４年１月１１日（２００２．１．１１）
【出願番号】特願２０００－１８２０１５（Ｐ２０００－１８２０１５）
【国際特許分類】
　G06F　13/00　　(2006.01)
　H04L　12/66　　(2006.01)
　H04L　12/22　　(2006.01)
【ＦＩ】
　G06F 13/00　　351 Z
　H04L 12/66　　B
　H04L 12/22

【手続補正書】
【提出日】平成１９年４月２６日（２００７．４．２６）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　通信路に介在され、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置。
【請求項２】
　データの検証および制御を行う主制御装置と、第１の通信路と接続された第１のバッファと、前記主制御装置に接続され要求またはデータを蓄積する第２のバッファと、前記第１のバッファと第２のバッファとを短絡・開放する第１のスイッチと、前記主制御装置と第２の通信路とを短絡・開放する第２のスイッチと、前記主制御装置からの指示により、前記第１または第２のいずれか一方のスイッチを排他的に短絡させるための制御信号を出力するスイッチ管制部とからなる通信路のスイッチ接続制御装置。
【請求項３】
　前記第１のバッファは、第１の通信路からの要求またはデータの正当性を検証する検証手段を備えた請求項１記載の通信路のスイッチ接続制御装置。
【請求項４】
　前記主制御装置は、第２の通信路からの要求またはデータの正当性を検証する検証手段を備えた請求項１記載の通信路のスイッチ接続制御装置。
【請求項５】
　前記に加えて、主制御装置と第２のスイッチとの間に要求またはデータを蓄積する第３のバッファと、前記第２の通信路と前記第２のスイッチとの間に要求またはデータを蓄積する第４のバッファとを備えた請求項２記載の通信路のスイッチ接続制御装置。